Cybercrime and Electronic Evidence

Kilby Baker

Australia's International Crime Cooperation Central Authority

Importance of Mutual Assistance

- Mutual assistance is the formal government to government process to obtain electronic evidence

- The evidence obtained as a result of mutual assistance is often critical in criminal proceedings or prosecutions

- Electronic evidence can show who owned an account that committed a criminal act or what criminals communicated about a crime

Obtaining Electronic Evidence

- Electronic evidence is commonly held on servers in foreign countries

- A mutual assistance request is required to obtain electronic evidence

- It takes a long time to obtain electronic evidence!
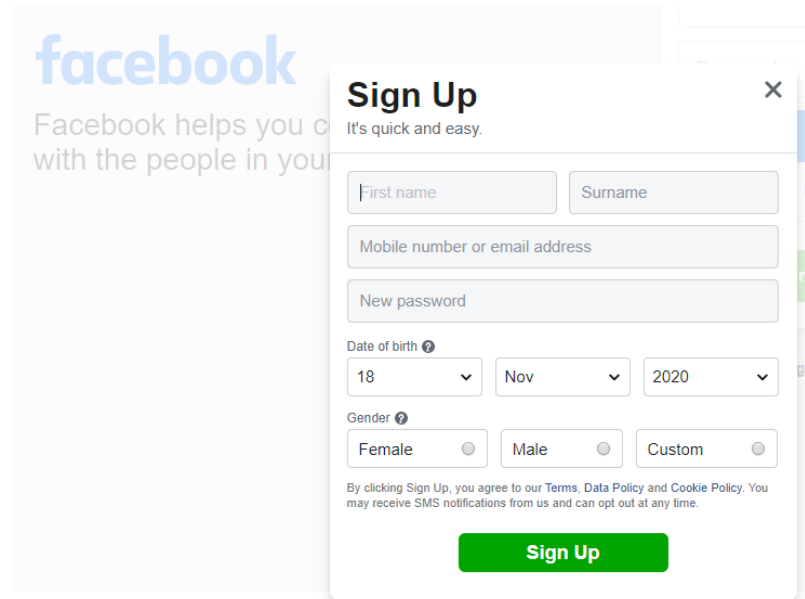
Types of Electronic Evidence

- Internet data is electronic evidence and may be:
  - Non-content data
  - Content data

- Internet data comes from communication service providers (CSPs)

Non-Content Data
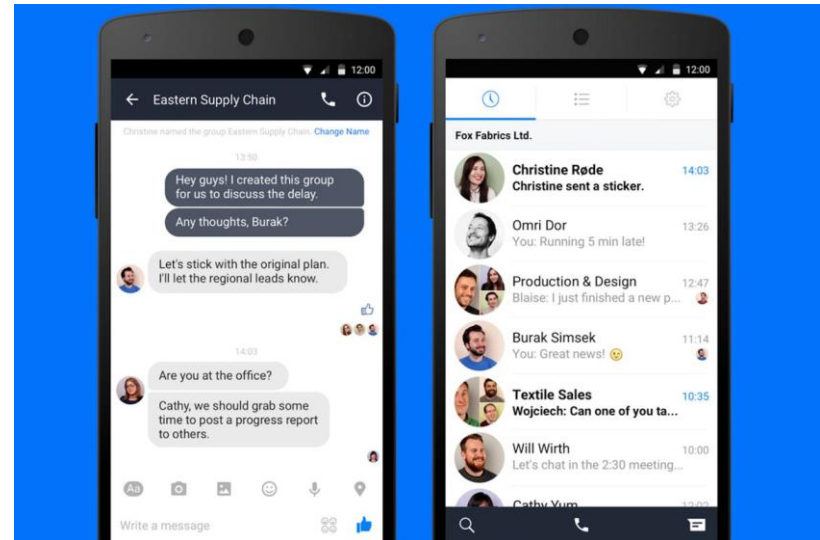
- Subscriber details associated with an account

- Name
- Email address
- Phone number
- Date of birth
- IP addresses

Content Data

- Includes the actual content of the account created by the user

- Photographs/videos

- Messages

- GPS location data

- Standard of 'Probable Cause'

Probable Cause

- In order to obtain content records from the United States, we need to meet the legal standard of 'probable cause'.

- Probable cause is a **higher** threshold than 'reasonable grounds to believe'

- In order to meet probable cause, a MAR will need to contain <u>specific</u> and <u>detailed</u> information '*sufficient to warrant a prudent person's belief that evidence of a crime would be found in the search*'
  - account active for time for which records are sought
  - account actively used in relation to the offending conduct.

- Reasonable grounds: offence committed / evidence in records

Geofence Requests

- Specific to Google

- Google can identify which devices were in a geographical location at a specific time

- You must have the geographical location

  and date and time of the offending

- Google will return a list of devices which

  were in the locations

Preservation Requests

- A preservation request is a 'snapshot' of an account which is saved by the CSP

- If a user deletes their account, the evidence will be preserved

- Make a preservation request **as soon as possible**

- Law enforcement are responsible for preservation requests

Portals/Service Providers

- CSPs have online portals for law enforcement to make preservation requests

- The portals are only for law enforcement

- CSPs do not send reminders

Law Enforcement Online Submissions

Oath's Law Enforcement Online Submissions (LEOS) system permits verified law enforcement agents and government officials to securely submit legal requests, including emergency disclosure requests in cases involving a danger of death or serious physical injury.

LEOS can be used to submit legal process for data held by Oath Holdings Inc. (formerly Yahoo) and Oath Inc.(formerly AOL).

Email address

Password

Log In

Forgot Password?

Don't have an account? Create New Account

YAHOO! AoI.

Timeframes

- The average timeframe to obtain electronic evidence is 9 – 12 months

- If a matter is urgent, let the foreign country know and explain why e.g. upcoming trial

- COVID-19 has impacted some countries ability to provide evidence